UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,108	07/27/2000	Tatsuya Fujiyama	TSM-13	2655

24956 7590 02/27/2004

MATTINGLY, STANGER & MALUR, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 02/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,108	FUJIYAMA ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to **a single paragraph** on a separate sheet **within the range of 50 to 150 words**. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The examiner notes that the abstract is currently 2 paragraphs in length and exceeds 150 words. Appropriate corrections are required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

The examiner will interpret the claims as best understood for applying the appropriate art for rejection purposes.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 and 5-16 are rejected under 35 U.S.C. 102(b) as being anticipated by the Internet Scanner User Guide (herein referred to as ISS). The examiner notes that the applicant's claim language is in bracketed form next to the equivalent recitations of the prior art teachings.

As per claim 1, ISS discloses of a CD-ROM that contains the Internet Scanner (program comprising a method) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network (system)) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (by a display unit connected to an electronic

computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) of the network (first specification system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (via a fourth step)(pg 69, 71).

As per claims 5 and 12, it is taught by ISS of database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). It is recited of reports being grouped into 4 categories (third specification) whereby executive reports handle top-level security issues (pg 69). The policy list comprises the scan types that are to be performed on the network (first specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81). It is interpreted by the examiner that the fixes and patches (collectively referred to as countermeasures) correspond to the executive reports as recited on page 69 and will not exceed the security level listed based on the type of report. The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting

the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input device) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claims 6 and 13, it is taught by ISS that the user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (first specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81).The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input device) whether the vulnerabilities are to be fixed or

patched (collectively referred to as countermeasures as read from the database)(pg 69, 71)

As per claims 7 and 8, ISS teaches of a CD-ROM (storage medium) that contains (stores) the Internet Scanner (program) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network (system))(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network (system)) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the

database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) of the network (first specification system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (via a fourth step)(pg 69, 71).

As per claim 9, ISS discloses of a CD-ROM that contains the Internet Scanner (security evaluation) that is installed on a computer (apparatus)(pg 15). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The user (operator) selects via a graphical user interface (input unit connected to the computer) the network (first specification accepting unit) to be scanned (evaluated) and the devices (second specification accepting unit of each of the components constituting the network/system)(pg 31,38, and 47). The policy list comprises the scan types that are to be performed on the network (specified first specification accepting unit) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed in a window based upon the scanning (evaluating) of the

devices (second specification accepting unit of each of the components constituting the network /system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting (via the third specification accepting unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed in a window based upon the scanning (evaluating unit) of the devices (second specification accepting unit of each of the components constituting the network/system) of the network (first specification accepting unit) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (state of security)(pg 69, 71).

As per claim 10, ISS discloses of a CD-ROM that contains the Internet Scanner (program comprising a method) that is installed on a (electronic) computer (pg 15). The Internet Scanner provides information (support making) about patches and fixes (collectively referred to as countermeasures) to a user (pg 69-71). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). Fixes and patches (collectively referred to as

countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claim 11, it is taught by ISS of database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (first specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81). It is interpreted by the examiner that the fixes and patches (collectively referred to as

countermeasures) correspond to the respective items listed on page 58-59 that are evaluated during the scan tests during the reading out from the database during a second step. The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the display) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claims 14 and 15, ISS teaches of a CD-ROM (storage medium) that contains (stores) the Internet Scanner (program) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network (system))(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that

are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claim 16, ISS discloses of a CD-ROM that contains the Internet Scanner (security construction support apparatus) that is installed on a computer (pg 15). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification accepting unit of each of the constituent components of the network) (pg 31,70, and 98). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The user (operator) selects via a graphical user interface (input unit connected to the computer) the network (first specification accepting unit) to be scanned (evaluated) and the devices (second specification accepting unit of each of the components constituting the network/system)(pg 31,38, and 47). The policy list comprises the scan types that are to be performed on the network by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed in a window based upon the scanning (evaluating) of the devices (second specification accepting unit of each of the components constituting the network) that were specified by the user

(operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (via a security countermeasure display unit) in a window based upon the scanning of the devices (second specification accepting unit of each of the components constituting the network/system) of the network (first specification accepting unit) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from memory) the detected vulnerabilities (state of security)(pg 69, 71).

Allowable Subject Matter

8. Claims 2-4 would be allowable if rewritten to overcome the rejection under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

As per claim 2, it was not found to be taught in the prior art of for each security type, determining the ratio of the number of security countermeasures accepted as executed to the number of security countermeasures classified into the security type concerned and displaying a degree of accomplishment of the security countermeasures classified into the security type.

As per claim 3, it was not found to be taught in the prior art of determining the total sum of degrees of risks corresponding to the security countermeasures accepted as non-executed out of the security countermeasures classified into a security type and displaying the total sum of the degrees of risk for each of the security types as a degree of the remaining risk of the security countermeasures classified into the respective security types.

As per claim 4, it was not found to be taught in the prior art of determining the total sum of the costs corresponding to the security countermeasures accepted as executed out of the security countermeasures classified into a security type and displaying the total sum of the costs for each of the security types as the required cost of the security countermeasures classified into the security type.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Townsend, U.S. Patent 6,631,473 Application of applying security countermeasures.

Kingsford et al, U.S. Patent 6,574,737 General use of vulnerability scanning and applying corrections to detected vulnerabilities.

Baudoin et al, US 2004/0010709 Determination of risks and applying ratings to security policies.

Bunker, V et al, US 2003/0056116 Percent reduction in vulnerabilities and lists risk levels.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

2/23/04

CR

February 23, 2004